

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA
LAFAYETTE DIVISION

UNITED STATES OF AMERICA : DOCKET NO. 6:18-185-1

VS. : JUDGE ZAINEY

DERRICK FELTON (01) : MAGISTRATE JUDGE HANNA

RULING AND REASONS

Before the Court is “Defendant’s Motion to Suppress Evidence” (Rec. 96). Defendant Derrick Felton moves to suppress all evidence obtained from the administrative subpoena issued by the FBI to Comcast Communications (“Comcast”) on or about November 27, 2017 and evidence obtained without a warrant from the United States Postal Service (“USPS”). Felton argues that he had a reasonable expectation of privacy as to the content of the communications between his IP address and the USPS server and the information obtained from Comcast regarding his IP address. Felton maintains that the government violated his Fourth Amendment rights because it failed to obtain a search warrant.

The government argues that the motion should be denied because; (1) Felton lacks standing to challenge the alleged searches, and (2) even if Felton had standing, the activities complained of do not constitute a search within the meaning of the Fourth Amendment.

The Indictment

Felton was indicted along with two other individuals for multiple drug

trafficking crimes including conspiracy to distribute and possess with intent to distribute methamphetamine. The facts that led to the indictment involved three (3) suspicious packages shipped from Los Angeles, California to Lafayette, Louisiana. A United States Postal Service employee observed the suspicious packages and contacted law enforcement. After an alert was made by a drug detection K-9, a search warrant was obtained and executed.

The three (3) packages contained approximately eighteen pounds of methamphetamine. Felton's fingerprints were on cooking pans found inside the packages. After further investigation, law enforcement was able to determine through financial records that Felton had been in Los Angeles, California during the time of the shipment. The investigation further revealed that Felton's IP address was used to check on the progress of the packages while in transit.

The Fourth Amendment

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."¹ A Fourth Amendment violation occurs in two (2) ways: (1) if the government action violates a person's "reasonable expectation of privacy . . . that society is prepared to recognize as reasonable,"² and (2) if the government "obtains information by intruding on a person's houses, papers, or effects."³ The protections of the Fourth Amendment apply only where there is a "subjective expectation of privacy . . . that

¹ U.S. Const. Amend. IX.

² *Katz v. United States*, 389 U.S. 347 (1967).

³ *United States v. Jones*, 565 U.S. 400 (2012); *see also Florida v. Jardines*, 569 U.S. 1 (2013).

society accepts as objectively reasonable.”⁴

The Information Provided by Comcast to the Government did not Violate Felton’s Fourth Amendment Rights

Internet connections are made via an IP address which identifies the computer and facilitates the orderly flow of electronic information on the Internet.⁵ The IP address provides the basic routing information a user needs to “contact and access a particular computer on the Internet, along with the website or other information stored thereon.”⁶

Felton used Comcast Communications (“Comcast”) as his Internet service provider. Comcast owns the IP addresses. Comcast issued a certain IP address to Felton in order for him to connect to the Internet.

Pursuant to its administrative subpoena power granted by 21 U.S.C. § 876, the FBI obtained subscriber information records in the custody and control of Comcast. Specifically, Comcast provided the government with the IP address that belonged to Felton—the same IP address used to track the three packages shipped from California to Louisiana. Comcast also provided the physical address of the person for which it assigned the IP address.

Felton argues that this was an intrusion on his personal property, including his paper and effects. The government argues that there was no constitutional violation because the information obtained (Felton’s IP address) was in the custody

⁴ *O’Connor v. Ortega* 480 U.S. 709, 715 (1987); *California v. Ciraolo*, 476 U.S. 207, 211 (1986); *Oliver v. United States*, 466 U.S. 170, 177 (1984); *Katz v. United States*, 389 U.S. 347, 361 (1961).

⁵ *United States v. Yu*, 411 Fed. Appx. 559, 560 n.1 (4th Cir. 2010).

⁶ *Peterson v. Nat’s Telecomm’ns & Info. Admin.*, 478 F.3d 626, 629 (4th Cir. 2007).

and control of a third party.

The government relies on *United States v. Miller*,⁷ where the Supreme Court held that “the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant, even if a criminal prosecution is contemplated at the time the subpoena is issued.” In *Miller*, the defendant moved to suppress microfilms of checks, deposit slips, and other records relating to his accounts at two banks. He contended that the subpoenas duces tecum pursuant to which the material had been produced by the banks were defective, and that the records had thus been illegally seized in violation of the Fourth Amendment.

The Court reasoned that there is no legitimate “expectation of privacy” in the content of the original checks and deposit slips because the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed to government authorities.

The Court finds that the subpoena issued in this case was issued to obtain third-party business records and thus, Felton had a reduced expectation of privacy. Furthermore, although not briefed by the Government, 18 U.S.C.A § 2703 permits disclosure of customer communications or records. More specifically, with respect to records concerning electronic communication service or remote computing services, § 2703 (c) provides as follows:

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the

⁷ 425 U.S. 435, 444 (1976).

governmental entity –

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the - -

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

Accordingly, Felton has failed to allege a violation of the Fourth Amendment as to the information (Felton's IP address and physical address) obtained from Comcast.

The Search of Communications and Property Held by USPS and Comcast Communications

When three (3) packages were shipped from California to Louisiana, the USPS assigned each package a tracking number. The sender or anyone who knew the tracking number had the ability to visit the USPS website and track the packages' progress while in transit.

Felton logged on to the www.usps.com website to track the packages shipped from California to Louisiana using each package's particular tracking number. By logging on to the USPS server, Felton was able to obtain information of the exact location of the packages and when they were delivered to their final destination.

The FBI searched and seized communications between Felton's IP address and the USPS server. Through discovery, the government obtained logs collected by the USPS which detailed the specific IP address that tracked the packages at a particular point in time. The IP address information also revealed the location of the individual tracking the package.

As stated above, the FBI also obtained subscriber information records in the

custody and control of Comcast; specifically, the FBI obtained the IP address used to track the shipments of methamphetamine. With this information, the FBI was able to determine that Felton's IP address was tracking the three packages as they were in transit from California to Louisiana, as well as the fact that when the IP address was issued by Comcast, the IP address was associated with Felton's residence in Sugarland, Texas.

Felton argues that the seizure of the communications from the USPS, without a search warrant, violated his Fourth Amendment rights, and that the administrative subpoena served upon Comcast to obtain Felton's IP address violated the Fourth Amendment.

Felton seeks to suppress the evidence the government obtained from the USPS and Comcast. The government argues that Felton does not have standing to challenge the legality of the alleged searches. The government argues that even if Felton had standing, the activities at issue do not constitute a search within the meaning of the Fourth Amendment because Felton cannot manifest a subjective expectation of privacy that is objectively reasonable regarding the information held and maintained solely by the USPS tracking system and by Comcast.

The concept of standing concerns "whether the person seeking to challenge the legality of a search as a basis for suppressing evidence was himself the 'victim' of the search or seizure."⁸ Fourth Amendment rights are personal that may not be asserted

⁸ *Rakas v. Illinois*, 439 U.S. 128, 132 (1978).

vicariously[.]”⁹ “A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person’s premises or property has not had any of his Fourth Amendment rights infringed.”¹⁰

The government argues that Felton lacks standing to challenge the alleged searches because he was not a “victim” of the search or seizure. The government posits that the information it obtained belonged to the USPS and Comcast. In other words, because the property belonged to USPS and Comcast, Felton is not a victim and therefore lacks standing to challenge the searches for failure to obtain a warrant.

Felton argues that the FBI’s acquisition of the content of the communications between Felton’s IP address and USPS was a search because Felton had a reasonable expectation of privacy in the communications occurring between his IP address and the USPS in the comfort of his residence. Felton posits that because the IP address was connected to his home, he had a reasonable expectation that the communications between his IP address and the USPS would not be interfered with by the FBI without a warrant.

Felton relies on *Carpenter v. US*,¹¹ which held that the government’s acquisition of defendant’s cell-site records from a wireless carrier was a Fourth Amendment search. The cell-site records allowed the government to obtain 12,898 location points cataloging defendant’s movements over 127 days. The Court recognized that individuals have a reasonable expectation of privacy in the whole of

⁹ *Id.* at 133.

¹⁰ *Id.* at 134 (citing *Alderman v. United States*, 394 U.S. 165, 174 (1969)).

¹¹ *Id.*

their physical movements.¹² The Court remarked that cell phone information is not truly “shared” as the term is normally understood noting that cell phones and services they provide are “such a pervasive and insistent part of daily life” that carrying one is indispensable to participation in modern society.¹³

The Court relied on its ruling in *United States v. Jones*,¹⁴ where it determined that the attachment of Global-Position-System (“GPS”) tracking device to a vehicle, and the subsequent use of that device to monitor a vehicle’s movements on public streets, was a search within the meaning of the Fourth Amendment.

The *Carpenter* Court also reasoned that a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user’s part beyond powering up.¹⁵

However, the Court warned that the *Carpenter* decision was a narrow one and did not express a view on matters not before it. Specifically, it does not disturb the application of *Smith*¹⁶ and *Miller*,¹⁷ or call into question conventional surveillance techniques, or address other business records that might incidentally reveal location information.¹⁸

The government argues that even if Felton had standing to challenge the law enforcement activities regarding the searches, these activities do not constitute a search within the meaning of the Fourth Amendment. The government is correct; the

¹² Citing *Riley v. California*, 573 U.S. ___, ___, 134 S.Ct. 2473, 2494-2495 (2014).

¹³ *Carpenter*, 138 S.Ct. at 2210.

¹⁴ 565 U.S. 400, 132 S.Ct. 945 (January 23, 2012).

¹⁵ *Id.*

¹⁶ *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577 (1979).

¹⁷ *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619 (1976).

¹⁸ *Carpenter*, 138 S.Ct. at 2210 (internal citation omitted).

IP address and tracking logs obtained from the USPS and Comcast were not owned, nor possessed by Felton. The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another.¹⁹

“Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so “for any extended period of time was difficult and costly and therefore rarely undertaken. For that reason, ‘society’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period of time.”²⁰ However, the Court in *Carpenter* concluded that because the cell-phone data allowed law enforcement to track Carpenter’s every movement and to retrace his whereabouts, it invaded Carpenter’s reasonable expectation of privacy in the whole of his physical movements.

Such is not the case here. There is no doubt that the IP address and tracking logs were obtained from a third-party. By identifying Felton as the IP address owner and analyzing the data obtained from the USPS server, the government was able to determine that Felton’s IP address requested tracking information, such as the location of the packages and the delivery to their final destination.

This Court finds that first, the third-party doctrine is relevant in part because Felton’s use of the IP address is not so closely related to his “home” that the Court can say that there is a privacy interest as to his papers and personal effects. Second,


¹⁹ *Id.* at 2210.

²⁰ *Carpenter*, 138 S.Ct. at 2217 (citations omitted).

the logs obtained from the USPS do not track Felton's every movement of every day; they only identify the fact that Felton was tracking the packages. The Court further recognizes the very narrow ruling in *Carpenter* and finds that it does not govern this case. Thus, the Court concludes that there was no reasonable expectation of privacy as to the information provided by Comcast (Felton's IP address) and the content of the communication between Felton's IP address and the USPS server. Accordingly,

IT IS ORDERED that Defendant's Motion to Suppress Evidence (Rec. #96) is hereby **DENIED**.

THUS DONE AND SIGNED in New Orleans, Louisiana on this 15th day of February 2019.



JAY C. ZAINES
UNITED STATES DISTRICT JUDGE